Sangfor Endpoint Secure

Release Notes

Product Version	3.5.36
Document Version	01
Released on	Dec. 06, 2022

Disclaimer

Products, services or features described in this document, whether wholly or in part, may be not within your purchase scope or usage scope. The products, services or features you purchase must be subject to the commercial contract and terms as agreed by you and Sangfor. Unless otherwise provided in the contract, Sangfor disclaims warranties of any kind, either express or implied, for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Unless otherwise agreed, this document is used for reference only, and all statements, information, and recommendations therein do not constitute any express or implied warranties.

Technical Support

For technical support, please visit: https://www.sangfor.com/en/about-us/contact-us/technical-support

Send information about errors or any product related problem to tech.support@sangfor.com.

About This Document

This document is the release notes of Sangfor Endpoint Secure(ES) version 3.5.36.

Intended Audience

This document is intended for:

- Network design engineers
- O&M personnel

Note Icons

English Icon	Description
⚠ DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
⚠ WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
⚠ CAUTION	Indicates a hazardous situation, which if not avoided, could result in minor or moderate injury.
⚠ NOTICE	Indicates a hazardous situation, which if not avoided, could result in settings failing to take effect, equipment damage, or data loss. NOTICE addresses practices not related to personal injury.
NOTE	Calls attention to important information, best practices, and tips. NOTE addresses information not related to personal injury or equipment damage.

Change Log

Date	Change Description
Dec. 06, 2022	This is the first release of this document.

Contents

1 Overview

1.1 New Features & Values

1. **Linux real-time protection added**: Improve the overall security protection capability on the Linux side.
2. Optimize the automatic fixing rate of 100% confirmed threats.
3. **Windows endpoint self-adaptive function added:** Convenient for users to read and use.
4. **Brand-new UI of macOS client**: Release the first version of the brand-new UI interface of macOS client, which mainly supports users to perform fast and full-disk virus scanning, manual processing of virus files, export of virus fixing logs, and other functions, which meets the core demands of user clients.
5. **macOS client self-adaptation in Chinese and English**: macOS clients can identify the system language for self-adaptation during the installation and deployment. It can flexibly and manually switch between Chinese and English after the installation.
6. **Antivirus scan task filtering added**: Filter through the endpoint antivirus scan status to find out the endpoint with abnormal scanning and perform a second antivirus scan.
7. **Endpoint password authentication for "trusted files" added**: the administrator can control the endpoint user's trusted file permission by enabling the endpoint **password authentication for "trusted files"**, to prevent the end users from trusting malicious files without the administrator's consent.
8. **User hot patching**:
   a) New user hot patching rules added.
   b) It prevents application vulnerabilities and adds a hot patching pop-up window when certain vulnerabilities are detected.
   c) Provide the attack logs regarding the exploit on endpoint application vulnerability. The log supports export and fuzzy query.
   d) Report the exploit on endpoint application vulnerability to MGR.

   e) Integrate into the UMH framework of the Security Capability Department.

9. **Proxy**: Endpoint Secure in the user's intranet environment can go online to update patches, virus databases, Neural-X, etc., through the proxy server.
10. **Advanced Threats**: **Advanced Threats** refer to collecting and analyzing endpoint behavior (such as file operation behavior, process operation behavior, network connection behavior, etc.) through the behavior detection engine (IOA, IOC). Based on the preliminary analysis results, certain behaviors will be aggregated to generate a security event for the administrator to analyze the attack process further using attack tracing (including attack sources, behaviors, and impacts).
11. **Threat hunting**: Supports multiple search conditions (including connections, domain name access, file operation, process operation, loaded module, and device information) to query endpoints with suspicious behaviors, accurately locate threats, and promptly remove residual files.
12. **Asset Attributes Optimization**: Users can specify the department of their endpoints based on the actual situation to solve the problem that automatic grouping based on IP addresses is not available when network segment conflicts exist among different departments.
13. **Custom size of quarantine space**: Supports custom size of quarantine space for both Windows and Linux endpoints. The size ranges from 1,000 MB to 100 GB.
14. **Custom IOC and exclusion policy added**:
    a) Support black and whitelists via custom file hash.
    b) Supports whitelisting files, directories, and suffixes
    c) Supports fuzzy matching and batch importing.

    You can respond quickly when false positives and false negatives are found, significantly improve the efficiency of operation and maintenance.
15. **Enhance the capacity of mining detection, traceability, and remediation**: The administrator can view detection details and remediation of cryptomining malware, such as persistent items and process memory, to trace cryptomining behaviors.
16. **File Identification via Neural-X**: Supports file identification based on big

data analytics, threat intelligence, and analysis by security experts to help customers analyze and fix security events, especially critical events.

17. **Forced Scan**: For some stubborn viruses that are difficult to deal with or cannot handle by customers (such as rootkits with strong resistance), **Forced Scan** can be distributed in batches on the management platform for fixing, improve the response speed, help customers quickly respond to large-scale infection with difficult-to-handle viruses, and improve customer satisfaction.
18. **Asset Inventory Optimization**: Added **Database Apps**, **Websites**, **Web Frameworks**, **Web Services**, and **Web Apps** information to understand the current status of server assets in a more refined manner and greatly improve asset management efficiency.
19. **Linux system Vulnerability Scanning**: To know what system vulnerabilities exist in the Linux endpoint.
20. **LDAP**: Support endpoints to synchronize AD domain user information and achieve automatic grouping of endpoints.
21. **Session Lock**: The administrator may lock the session at any time to avoid misoperation by others if the administrator is away.
22. Non-super administrators need to forcibly change their passwords when they first log in to their accounts.
23. **P2P Distribution**: Solve large-scale deployment issues for customers with the problem of limited platform components, inability to perform large concurrent pushes, and limited promotion speed.
24. **Development Environment Identification**: Can identify the development environment and its security. ES will only give alerts on the risk behaviors from identified secure files, avoiding freezing issues, false positives, and other impacts. At the same time, it can minimize the vulnerabilities of trusting files, help administrators effectively implement endpoint security planning, and alleviate security risks caused by security software.

25. **Smart Adaptive Antivirus Scanner**: During scanning, the CPU usage is intelligently adjusted according to the endpoint adaptation situation to ensure that the endpoint business does not get interrupted. According to

the endpoint's current total CPU usage, the antivirus process's CPU occupied is dynamically adjusted from 5% to 70%.

26. **Enables Realtime Protection under compatibility mode**: When an end user installs an antivirus that is not on the compatibility list, the Endpoint Secure client will receive an alarm and inform the customer of the risks of the installation in advance. The end user can understand the logic and risks of disabling real-time protection. The administrator can view the real-time monitoring status of the endpoint. When the real-time monitoring of the endpoint is disabled due to incompatibility, the administrator can enable the real-time monitoring function for the endpoint.
27. **Name and Logo Customization**: Satisfy the personalized needs of customers and government agencies.
28. Other functions optimization:
    a) **Response** > **Endpoints** displays all endpoint's security events, including Webshell Backdoor, Advanced Threats, Brute Force Attacks, PowerShell, and Botnet.
    b) The number of threat files processed in a single batch has been increased from 500 in the previous version to 10,000.
    c) Windows 10 endpoint environment fixed. Fix the issue that Sangfor Endpoint Secure and Windows defender notifications pop up during virus database updates.
    d) The built-in whitelist parameters of PowerShell increase to 200, and the built-in and custom parameters increase to 500.
    e) Optimize the virus-fixing task experience.
    f) Support Windows 11 operating system.
    g) The Endpoint Secure Management can view the trust file added by the endpoint.
    h) Optimize the File-trust operation user experience.

1.1.1 Others

None.

1.1.2 Integration with Third-Party Products

None.

1.2 Update Impacts

The service will restart after the update. However, restarting the device is not required.

1.2.1 Impacts on Services

During the update process, events detected on the ES agent cannot be reported to Endpoint Secure Manager.

1.2.2 Impacts on O&M

Endpoint Secure Manager cannot be logged in for 10 minutes.

1.2.3 Impacts on Customer Network

The update of Endpoint Secure Manager may take 10 minutes. The update time of Endpoint Secure agents depends on the number of agents.

NOTE

The maximum bandwidth of downloading agents is 2 MB/s, and the maximum number of agents in a download task is 5. Therefore, it will take 5 minutes to download five agents under stable network conditions.

1.2.4 Other Impacts

None.

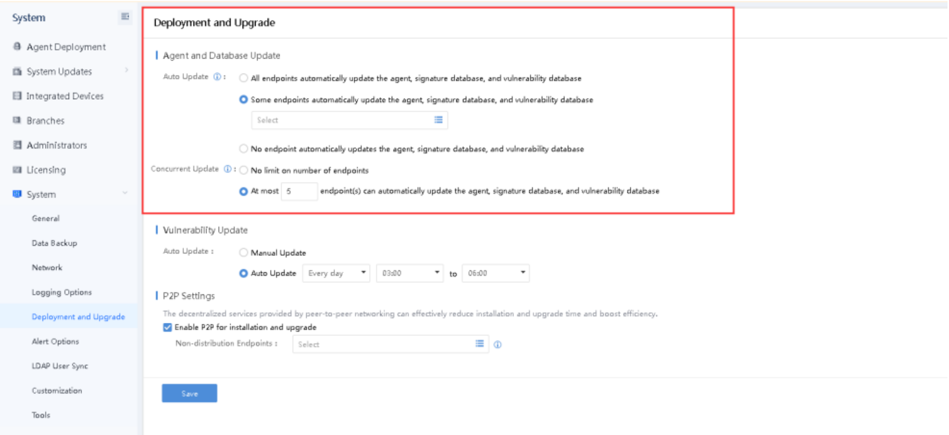
1.3 Customer Update Preparations

1.3.1 Update Preparations

The Endpoint Secure Manager needs to be updated.

1.3.2 Notes

If there are many endpoints, it is recommended to set some endpoints to upgrade first before upgrading the Endpoint Secure Manager, if no issue is found after some endpoints upgrades, you may upgrade all endpoints, as shown below:



Deployment and Upgrade

Agent and Database Update

Auto Update :
○ All endpoints automatically update the agent, signature database, and vulnerability database
● Some endpoints automatically update the agent, signature database, and vulnerability database
Select
○ No endpoint automatically updates the agent, signature database, and vulnerability database

Concurrent Update :
○ No limit on number of endpoints
● At most 5 endpoint(s) can automatically update the agent, signature database, and vulnerability database

Vulnerability Update

Auto Update :
○ Manual Update
● Auto Update Every day 03:00 to 06:00

P2P Settings

The decentralized services provided by peer-to-peer networking can effectively reduce installation and upgrade time and boost efficiency.
☑ Enable P2P for installation and upgrade
Non-distribution Endpoints : Select

Navigate to **System > System > Deployment and Upgrade**.

For **Auto Update**, select **Some endpoints automatically update the agent, signature database, and vulnerability database**.

For **Concurrent Update**, select **At most x endpoint(s) can automatically update the agent, signature database, and vulnerability database.**

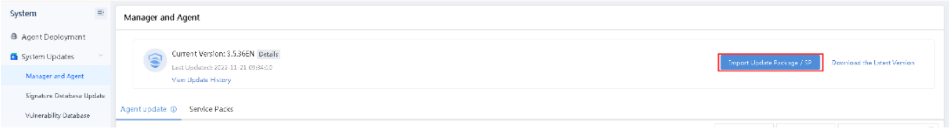
NOTE

The recommended number of concurrent updates of the endpoint is 5. However, you may adjust the number according to the actual need and situation.

1.4 Implementation Procedure

Offline Update:

Step 1. Navigate to **System** > **System Updates** > **Manager and Agent** and click **Import Update Package / SP** to import an update package.



Current Version: 3.5.36EN

Last Updated: 2022-11-21 09:34:10

Step 2. Perform the update. The update will complete in 10 minutes.

1.5 Post-Update Service Check

1. Able to log in to Endpoint Secure Manager.
2. Virus scan tasks sent can be completed.

1.6 Rollback Instructions

Rollback: Not supported.

(Contact a Sangfor technical support representative if the update fails) Rollbackis not supported. You can contact a Sangfor technical support representative to recover the Manager from the backup.

2 Update Guide

2.1 Preparations for Update

2.1.1 Update Tools

ES3.5.36EN update package: **ES3.5.36EN_20221201.pkg**

2.1.2 Environment Information

The update requires the Manager's IP address, username, and password.

2.1.3 Customer Resource Coordination

The update takes about 10 minutes. If the update fails, a server backend account and password are needed.

2.2 Pre-Update Check

Check whether the current version can be updated.

Current Version	Update Path	Notes
3.2.22EN-3.5.15EN	Any version of 3.2.22EN to 3.5.15EN > ES3.5.36EN_20221201.pkg	3.2.22EN, 3.5.5EN, 3.5.10EN, 3.5.15EN can be updated to 3.5.36EN.

2.3 Notes

- **Update Limitations**

The size of free disk space must be more than three times the size of the update package.

- **Immediate Update of Configurations, Logs, and Data**

Yes.

- **Update Recommendations**

1. During the update, do not restart the device manually and keep the device powered on.
2. If any error message pops up during the update, please do not perform any operations and call us at +6012-7117129 (7511) immediately. Do not manually restart the device.

- **Impacts of Central Management (CM) on Cluster**

None.

- **Pass-Through Supported**

Not supported.

- **High Availability Supported**

Not supported.

2.4 Update Procedure

2.4.1 Update Path

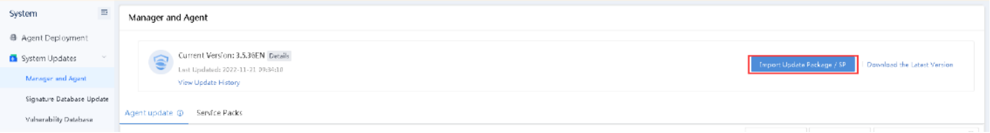
An update may take 15 minutes. Please perform the update during non-peakhours.

Update of custom versions is not supported.

Current Version	Update Path	Notes
3.2.22EN-3.5.15EN	Any version of 3.2.22EN-3.5.15EN -> ES3.5.36EN_20221201.pkg	3.2.22EN, 3.5.5EN, 3.5.10EN, 3.5.15EN can be updated to 3.5.36EN.

2.4.2 Update Procedure

Step 1. Navigate to **System > System Updates > Manager and Agent** and click **Import Update Package / SP** to import an update package.



Current Version: 3.5.36EN

Last Updated: 2022-11-21 09:34:10

Step 2. Perform the update. The update will be complete in 10 minutes.

2.5 Post-Update Check

2.5.1 Platform

Log in to the Manager and check whether the current version is 3.5.36EN by navigating to **System > System Updates > Manager and Agent**.

2.5.2 Service Status

Check whether the virus task sent can be completed.

2.6 Update Fails Troubleshooting

Contact a Sangfor technical support representative to troubleshoot.

2.7 Rollback Instructions

Rollback: Not supported.

(Contact a Sangfor technical support representative if the update fails). You can contact a Sangfor technical support representative to recover the Manager from the backup.

SANGFOR